

「地方公共団体における情報セキュリティポリシーに関するガイドライン（改定案）」に対する意見

2022年1月 24日

BSA｜The Software Alliance (BSA |ザ・ソフトウェア・アライアンス [1]、以下、「BSA」）は、総務省の「地方公共団体における情報セキュリティポリシーに関するガイドライン（改定案）」（以下「本ガイドライン」）に対するパブリック・コメントの機会に感謝し、以下のとおり意見を提出致します。

総論

BSA は、地方公共団体のサイバーセキュリティのレベルを統一的に向上させようとする貴省の不断の努力に感謝致します。BSA の会員企業は、クラウドコンピューティング、セキュリティソリューション、データアナリティクス、AI（人工知能）など の最先端の技術やサービスを世界に先駆けて提供し、政府や社会のデジタルトランスフォーメーションを支えています。サイバーセキュリティやデータ・ガバナンス政策の策定において、BSA は世界中の政府と緊密に協働してきました。そのことを通し、このような政策や法案が市民のプライバシーと自由を守りながら、サイバーセキュリティの脅威を効果的に抑止・管理するのを可能にするのを直に見てきました。

サイバーセキュリティ関連政策を成功させるための重要な要素として、国際的に認知された基準との整合性、リスクベース、成果志向、技術中立的アプローチの採用、イノベーション促進のために政策の順応性を高めることなどが挙げられます。そして、サイバーセキュリティ課題に対処するには、接続環境にあるデータ・エコシステムの完全性、機密性、回復力を防御するための革新的なツールと実践が必要であり、高度な暗号化など、最善のセキュリティソリューションを利用できることが不可欠です。したがって我々は、政府が民間部門と密接に協力し、セキュリティアプローチの最新の進歩の恩恵を受けられるように、セキュリティポリシーを策定することを奨 めます。

提言

デジタル社会の実現に向けた取り組みが加速する中、デジタル庁から発表された新たな「重点計画」[2]を我々は高く評価しています。本計画では、地方公共団体の情報システムを刷新する

---

[1] BSA の活動には、BSA’s members include: Adobe, Altium, Alteryx, Amazon Web Services, Atlassian, Autodesk, Aveva, Bentley Systems, Box, Cisco, CNC/Mastercam, CrowdStrike, Dassault, DocuSign, Dropbox, IBM, Informatica, Intel, MathWorks, Microsoft, Nikon, Okta, Oracle, PTC, Rockwell, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.が加盟企業として参加しています。詳しくはウェブサイト（http://bsa.or.jp）をご覧ください。

[2] 「デジタル社会の実現に向けた重点計画」
https://cio.go.jp/sites/default/files/uploads/documents/digital/20211224_policies_priority_package.pdf

22F Shibuya Mark City West
1-12-1 Dogenzaka Shibuyaku,
Tokyo 150-0043

P +81 3 4360 5473
F +81 3 4360 5301
W bsa.org

Japan Representative Office

政府の確固たるコミットメントが示され、デジタル変革のためには、安全なクラウドコンピューティングサービスを最大限に活用することが重要であることが認識されており、また、現在、ガバメントクラウド[3]を検証する先行事業が一部の地方自治体で実施されています。市民サービス向上のために、パブリッククラウドの利用拡大を視野に入れながら、貴省がデジタル庁と共に、ガイドラインを継続的に見直されることを我々は強く推奨します。

マイナンバーのネットワーク保護のためのクラウド活用推進

今回のガイドラインは、先般、内閣サイバーセキュリティセンター（NISC）が改訂した「政府機関等のサイバーセキュリティ対策のための統一基準」[4]との整合性を図ることに重点が置いていていると理解しています。クラウドサービスが「外部サービス」に含まれ、取り扱う情報の機密性に基づいたセキュリティ対策が推奨される等、ガイドラインにおいて明確化されたことを我々は支持します。また、クラウドサービスの選定において、国際的に認められたセキュリティ基準や第三者監査が認められていることも歓迎します。

本ガイドラインにおける上記の改善点を高く評価しつつも、我々は、場合によっては物理的なネットワーク分離を必要とするような、現在の「三層の対策」に依存しないセキュリティアプローチを継続的に検討されることを強く推奨します。BSA 会員のクラウドサービスは、インターネットを介した信頼性の高い安全なアクセスを可能にする世界で最も安全なインフラに支えられており、暗号化、ゼロトラストアーキテクチャ、高度アクセス管理などの国際的に認められた機能により、機密性の高い個人情報の安全な取り扱いを実現しています。機密性の高い個人情報やその他のデータを保護するための最も効果的なデータセキュリティソリューションは、これらのクラウドサービスによって提供されているのです。

このような視点から、現行の LGWAN をインターネットに接続された情報システムから分離する現在のセキュリティ・アプローチを見直されることを求めます。この物理的な分離により、LGWAN を使用する政府機関は、クラウドコンピューティングの高度なセキュリティと機能を十分に活用することができなくなってしまいます。貴省が有用であるとお考えであれば、この点に関する理解を深めるために、インターネット接続構成環境におけるセキュリティ確保に関する、BSA 会員による技術セッションを開催することも可能です。

我々は、地方公共団体がマイナンバーのデータ管理のための情報システムを保護する必要性を全面的に支持します。しかし、世界中の公共機関においては、情報セキュリティが最も必要とされる業務においてさえも、クラウドサービスが利用されています。信頼性、セキュリティ、拡張性、コスト削減、スピード、アクセスや利用のしやすさなど、高品質のクラウドコンピューティングサービスがもたらす多くの利点が認識されているのです。クラウドサービスは、AI や IoT（Internet of Things - モノのインターネット）、その他の先端技術を用いたイノベーションを可能にします。貴省が本ガイドラインをさらに更新し、日本における政府機関が上記のクラウドサービスの恩恵を享受できるようにすることを奨めます。

場所でなく、データセキュリティ実践に基づくクラウドサービスプロバイダ（CSP）の選定

また、外部サービスの利用に関する本ガイドラインの説明が、日本国外のサーバにデータを保存・ 処理する可能性のある CSP の利用を不必要に制限しているように読めることを、我々は引き続き懸念しております。データセキュリティの確保は、CSP が維持する技術的・物理的なセキュリティ管理に依存しており、データセンターの存在地は、CSP がどのように個人情報を保護するか又は利用者に適用される法律を遵守するかには、ほとんど関係がありません。実際、クラウドサービスの利点の多くは、国境を越えてデータが移転できることにあります。

[3] https://www.digital.go.jp/policies/posts/gov_cloud
[4] https://www.nisc.go.jp/active/general/pdf/kijyunr3.pdf

地理的に分散した複数のデータセンター間でデータを移転し、冗長的に保存することでレジリエンス（弾力性）が高まり、データのセキュリティは向上するのです。このアプローチは、日本政府が提唱する「データ・フリー・フロー・ウィズ・トラスト（DFFT）」と明確に合致しています。それゆえに、物理的な場所に焦点を当てた本ガイドラインは、そのような移転を制限することになり、実際には地方公共団体が扱うデータのセキュリティを損なう可能性があります。

以上を踏まえ、貴省に対し、外部サービスの選定の箇所について、以下のように修正することを求めます。

（iii-148 頁）
第３編：地方公共団体における情報セキュリティポリシー（解説）
第２章 情報セキュリティ対策基準（解説）
8. 業務委託と外部サービスの利用
8.2 外部サービスの利用（機密性 2 以上の情報を取り扱う場合）
（２）外部サービスの選定

「② インターネットを介して提供される外部サービスの利用に当たっ ては、外部サービス提供者の事業所の場所に関わらず、データセンターの存在地の国の法律の適用を受ける場合があることに留意する必要がある。具体的には、外部サービス提供者のサービスの利用を通じて海外のデータセンター内に蓄積された地方公共団体の情報が、データセンターの設置されている国の法令 により、日本の法令では認められていない場合であっても海外の当局による情報の差し押さえや解析が行われる可能性があるため、~~日本の法令の範囲内で運用できるデータセンターを選択する必要がある。~~**日本の法令を遵守した場所・方法でデータが保管されることを保証できるサービスプロバイダが運用するデータセンターを選択する必要がある。**」

さらに、ガイドラインの 8.2 の（解説）（２） ⑤ では、地方公共団体が外部サービス提供者のセキュリティを保証するために、国際的に認められた様々な規格やその他のプログラムに基づく監査または監査報告書や認証に依拠するなど、一定の選択措置を推奨しています。この中には、ISO/IEC 27017 や政府情報システムのためのセキュリティ評価制度（ISMAP）、日本セキュリティ監査協会のクラウド情報セキュリティ監査や SOC 報告書（Service Organization Control Report）などが含まれています。地方公共団体が利用できるセキュリティ保証について、貴省が柔軟性を持たせていることを我々は高く評価します。地方公共団体がサービスや委託先の信頼性を判断する際に参考とする選択肢として、これらの認証・管理基準・監査要件が記載されており、すべてを満たす必要は無い、という点を明確化することを奨めます。

以上を踏まえ、貴省に対し、以下のように修正することを求めます。

（iii-149-150 頁）
第３編：地方公共団体における情報セキュリティポリシー（解説）
第２章 情報セキュリティ対策基準（解説）
8. 業務委託と外部サービスの利用
8.2 外部サービスの利用　（機密性 2 以上の情報を取り扱う場合）
（２）外部サービスの選定

「⑤情報セキュリティ管理者は、外部サービスに対する情報セキュリティ監査による報告書の内容、各種の認定・認証制度の適用状況等から、外部サービス及び当該 サービスの委託先の信頼性が十分であることを総合的・客観的に評価し判断しな ければならない。.........
このような評価に当たって、外部サービス提供者が利用者に提供可能な第三者による監査報告書や認証等を取得している場合には、その監査報告書や認証等を 利用する必要がある。

22F Shibuya Mark City West
1-12-1 Dogenzaka Shibuyaku,
Tokyo 150-0043
P +81 3 4360 5473
F +81 3 4360 5301
W bsa.org
Japan Representative Office

なお、選定条件となる認証には、ISO/IEC 27017 によるクラウドサービス分野 における ISMS 認証の国際規格がある。また、ISMAP の管理基準を満たすことの 確認や ISMAP クラウドサービスリスト等のほか、日本セキュリティ監査協会のクラウド情報セキュリティ監査や外部サービス提供者等のセキュリティに係る内部統制の保証報告書である SOC 報告書（Service Organization Control Report）を活用することを推奨する。**上記の一つ又はそれ以上を参考とし、個別の案件に応じ、他の適切な認証やセキュリティ上の保証を利用することも可能とする。**」

また、貴省の本改定ガイドラインの概要[5]で示されているように、外部サービス提供者が満たすべきセキュリティ保証要件についての柔軟なアプローチを、中央政府においても採用されることを奨めます。ISMAP は、NISC、デジタル庁、経済産業省、総務省による共同運用であることは認識しておりますが、中央省庁の情報セキュリティ認証に関しても、貴省が主導し、同様の柔軟な対応を実施することを推奨します。

官民連携によるセキュリティ対策の刷新

テレワークが増加し、web 会議サービス利用が急増したことによるセキュリティへの影響を考慮した対応を本ガイドラインが提示していることを支持します。

より効果的なガイドラインとするために、上記に加え、ますます深刻化するランサムウェアへの対策にも言及することを奨めます。対策に関しては、様々な機関や団体が取り組みを公表しています。[6]ガイドラインの中で本情報を参照・活用することを推奨します。

また、サイバーセキュリティ対策のコンセンサスを形成するために、政府と産業界が強固なパートナーシップを築くことを強く支持します。サイバーセキュリティの解決策は、官民連携を受け入れ、市場主導型の解決策を促進することで、最も効果的となります。BSA と会員企業は、貴省と協働し、セキュリティアプローチの最新の進歩に関する洞察を共有していけることを期待しています。

結語

BSA は、本ガイドラインに対し意見する機会を頂けたことを感謝致します。提案された対策案に関し、利害関係者間で検討・議論をするための十分な時間を確保する上でも、今後は、少なくとも 30 日間の意見募集期間を設けることを強く希望します。今回の我々の意見が本ガイドラインを完成させる上で有益であることを願っております。日本のデジタルトランスフォーメーションの実現に向け、貴省を引き続き支援していきたいと我々は考えております。本意見について、ご質問、又、詳細について協議の機会を頂けるようでしたら、いつでもご連絡ください。

[5] https://www.soumu.go.jp/main_content/000785574.pdf (スライド10)
[6] https://security-portal.nisc.go.jp/stopransomware/